The Survivability Analysis Framework (SAF)

Carol Woody Ph.D. (presenter)
Robert Ellison Ph.D.

CERT
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **01 OCT 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE
The Survivability Analysis Framework (SAF)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

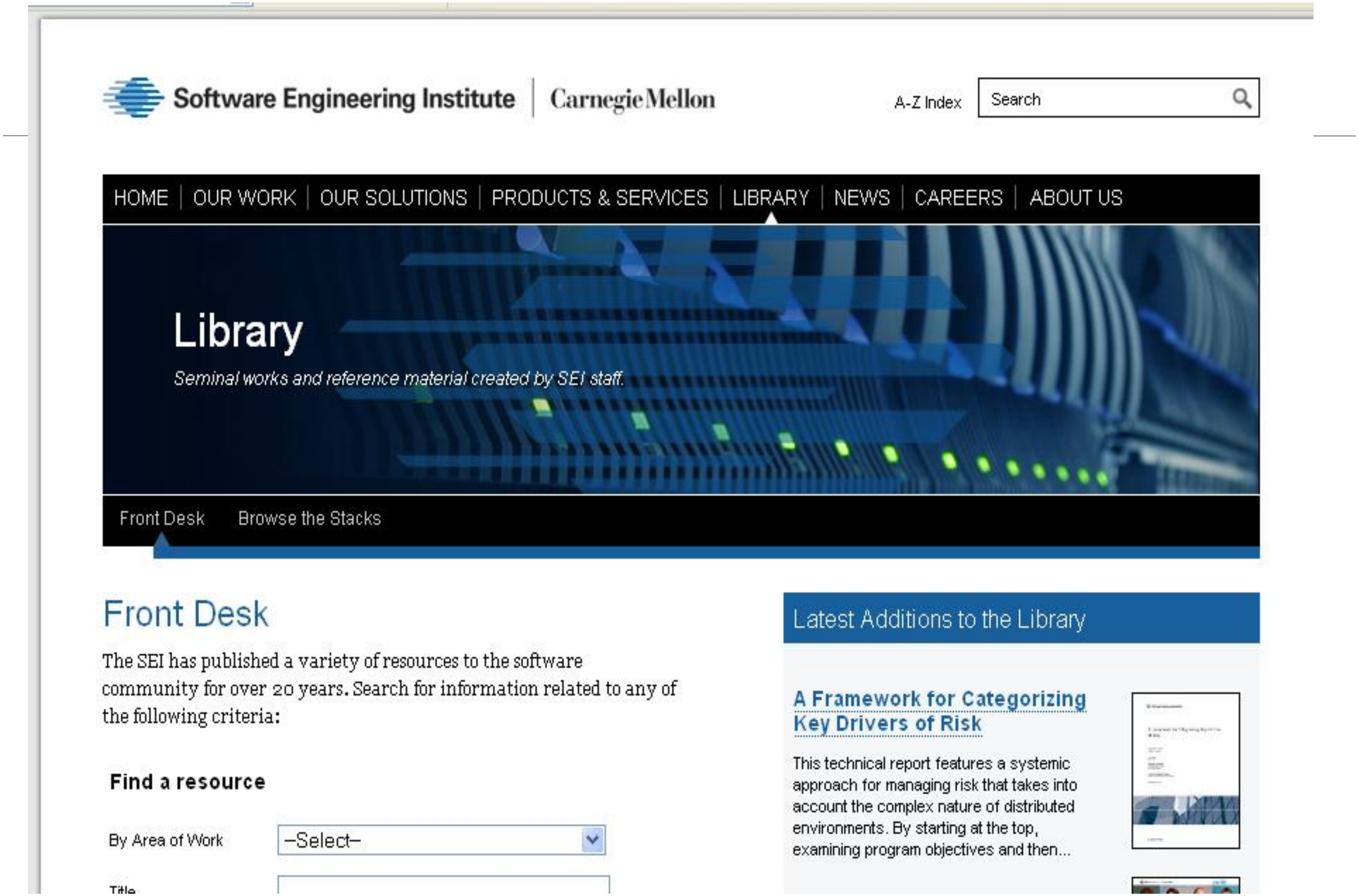
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**48**	


Software Engineering Institute | Carnegie Mellon
A-Z Index
Search
HOME | OUR WORK | OUR SOLUTIONS | PRODUCTS & SERVICES | LIBRARY | NEWS | CAREERS | ABOUT US
Front Desk
Browse the Stacks

Library

Seminal works and reference material created by SEI staff.

Front Desk

The SEI has published a variety of resources to the software community for over 20 years. Search for information related to any of the following criteria:

Find a resource

By Area of Work: –Select–

Title

Latest Additions to the Library

A Framework for Categorizing Key Drivers of Risk

This technical report features a systemic approach for managing risk that takes into account the complex nature of distributed environments. By starting at the top, examining program objectives and then...

About Carol Woody

Sr. Member of the SEI Technical Staff

Leads a team in CERT addressing critical gaps in assurance and survivability

25 years of experience in software management, acquisition, development, and implementation in large complex organizations

Polling Question 1

How did you hear about this webinar?

- Email invitation from the SEI
- SEI Website
- Website with webinar calendar (ie www.webinar-directory.com)
- Social Media site (LinkedIn, Twitter)
- Other

Why a Framework

The framework was developed to address the following research questions:

How can mission survivability be maintained as interoperability of systems increases?

Research sponsored by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD [AT&L])

How can operational impacts (such as information security) be tied to technology changes in operational mission execution?

U.S. Air Force’s Electronic systems Center (ESC) Cryptologic Systems Group (CPSG)

Piloted in 8 complex operational environments

Framework Description

Purpose of the Framework

Establish an approach for assembling the broad range of operational information (technology, people, and processes) to analyze it for survivability

- Failure responses must be planned – unexpected usage (malicious or accidental) that drives operational execution outside of expected behaviors
- Survivability must be considered within the context of other quality attributes (performance, usability, etc.)
- Complexity and change are unavoidable so inconsistencies (mismatches) must be assumed as we compose technology, people, and processes
- Operational compositions span organizational and technology boundaries

Change is Always Occurring

Survivability must accommodate the usual and the unexpected

Usual problems

- Power and communication outages
- Snow storms
- Staff illness & death

Expected changes

- New technology insertion
- Technology refreshes
- Location moves
- Operational security

Catastrophe is a matter of scale

Polling Question 2

What is your organization’s most critical operational concern?

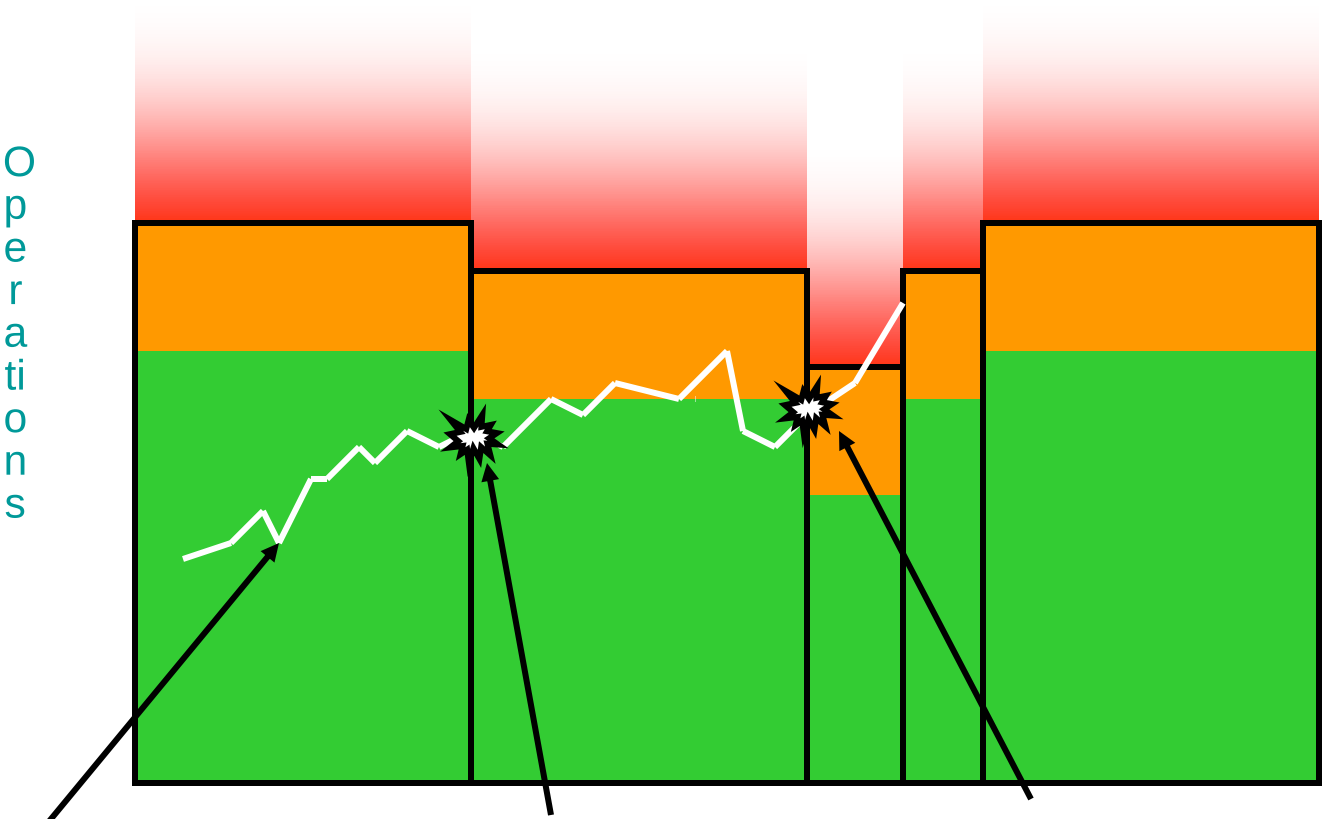
a) Continuity of operations

b) Natural disaster response

c) Contractual compliance

d) Vulnerability management

Failure Model of Catastrophe



EVENT

A failure or change

Increase in work load or usage

Reduction in capacity

Activity

An event edges system state closer to Orange zone.

A second event followed by increased usage pushes state towards Red.

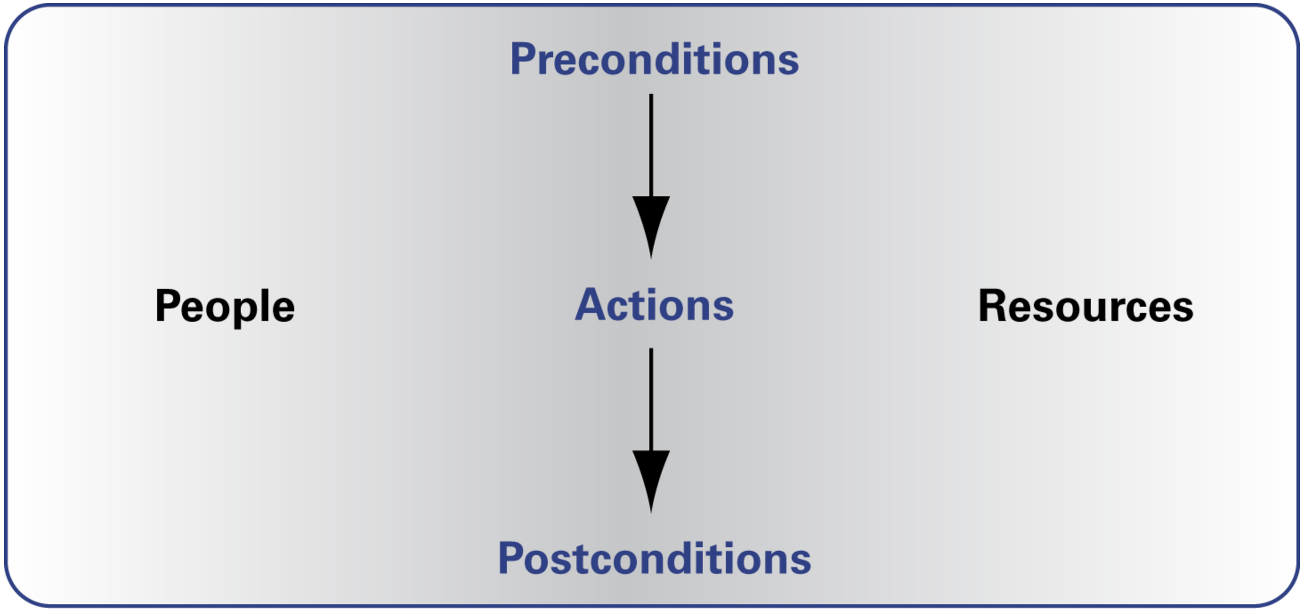
Survivability Analysis Framework (SAF) - 1

Framework for operational survivability analysis

Process:

- Select a critical business process for detail analysis
  - specific example of people applying technology to perform an operational mission
- Identify operational success criteria
- Describe critical steps in depth
  - Sequenced activities
  - Participants
  - Resources
- Identify and analyze ways critical steps may not function as intended and opportunities for mitigation

Survivable Analysis Framework (SAF) - 2



Stresses → **Acceptable Outcomes**

Analysis

- *Potential failure conditions*
- *Likelihood of error conditions*
- *Impact of occurrences*
- *Recovery strategies*

People and Resources

People can include

- direct performers of operational actions
- data entry, inquiry, verification, audit, synthesis among multiple information sources, administration for technology components, authentication and authorization authorities

Resources can include

- hardware—servers, data storage devices, PCs, PDAs, routers, telephone switches, satellite relays, physical access controls, and similar devices
- software—operating systems for each hardware platform, configuration management, databases, firewalls, network protocols, packet switches, authentication packages, Web applications, local and remote procedures
- policies and practices—certification and accreditation, third-party access management, outsourcing
- contracts, governance controls, and the like

Polling Question 3

Do you analyze the operational survivability of your critical business processes (missions)?

a) Yes

b) No

Example 1: Doctor Orders Blood Test

Simple example to show the structure of information used in SAF

Focus on failure analysis

Mission Thread Examples

Example 1: Scenario Steps

A. Patient brought to emergency room with chest pains.

B. Dr. Emergency reviews available records

C. Dr. Emergency develops a treatment plan.

D. Dr. Emergency orders series of blood tests.

E. Phlebotomist from laboratory arrives to collect first specimen which is sent to the lab.

F. Lab receives specimen, performs centrifuge and delivers serum to appropriate testing stations.

G. The Lab system notifies the ordering system that the specimen has been received for testing.

Example 1: Operational Context

Doctor is using a handheld device to review patient records, to record information during the exam, to order tests, and to receive test results.

The Lab is a separately run business that has contracted to provide services to all of the local hospitals.

For privacy purposes, the Lab does not have patient-specific information. The Lab bills the hospital, and the hospital bills the patient.

Example 1: Time-line of Actions - People

Describe how each person/organization is involved in each step and who has controlling authority (C)

Action People	A: Emergency Room Encounter	B: Doctor reviews patient records	C: Doctor develops treatment plan	D: Doctor orders blood tests	E: Phlebotomist arrives and take specimen
Patient	C				X
Doctor	X	C	C	C	
Lab Phlebotomist					C
Lab Technician					

Example 1: Time-line of Actions - Resources

Describe the resources involved in an action

Action **Resources**	A: Emergency Room Encounter	B: Doctor reviews patient records	C: Doctor develops treatment plan	D: Doctor orders blood test
Handheld device		X	X	X
Hospital Communication Hub		X	X	X
Hospital Admissions	X			
Hospital medical records		X	X	
Hospital Lab communications				X
Lab Systems				X

Example 1: Describing a Critical Step

Step D	**Doctor orders blood tests**
Precondition	Treatment plan defined Required lab tests identified Handheld connectivity to Lab Dr. E. authorization to order tests for this patient
Action	Enter order on handheld Order accepted, verified, and accepted by Lab
Post-Condition	Test confirmed and scheduled

Example 1: Failure Outcomes for Step D

Missing (or delayed) results:

- some or all tests are not done

Wrong results:

- some unrequested tests were performed
- results do not reflect the actual sample

Disclosure:

- results are disclosed to unauthorized person
- test results are not associated with the correct patient
- test results are not associated with the correct doctor

Example 1: Causes of Failure

Failure: Missing test results

- Paperwork requiring tests to be run was lost or misplaced
- Blood samples were lost, contaminated, or misplaced
- Some tests were not run by the technician
- Wrong tests were run by the technician
- Some or all test results were not associated with the correct patient by the lab
- Some or all test results were not associated with the right doctor by the lab
- Testing machine did not produce results
- Testing machine was not working and could not produce results

Example 2: Joint Military Operation

Complex example to show how the SAF structuring of information supports analysis

Focus on the impact of technology change on operational survivability

Example 2: Military Joint Forces Mission Thread

An army unit on patrol spots a missile launcher preparing to fire. The unit calls their commander and provides a description of the launcher and its location. Even though the launcher is in the Army’s area of responsibility, in this scenario the Army does not have an appropriate weapon to bring to bear (for example, the artillery could be in use on other targets). However, the Air Force has a suitable platform and is tasked as Executive Agent to further prosecute or strike of the target. The Army remains the authority for the strike even though the Air Force will perform the engagement.

Example 2: Scenario Steps

1. Army unit sees “something” (e.g. Missile launcher preparing to fire.)
2. Unit calls their command post via satellite connection and provides a description of the launcher and its location.
3. UAV is moved into position to evaluate the potential target.
4. Army Command notifies Joint Services of a critical target requesting approval and support
5. Joint Services approves the target for critical support
6. Joint Services review weapon(s) and delivery platform options based on timing, collateral damage, desired effect, etc.
7. Air Force plane selected to attack target
8. Order transmitted to pilot (usually verbally)
9. Pilot executes attack coordinated by JTAC (ground resource embedded in Army unit)
10. Multiple assessments lead to unified battle damage assessment (BDA)

Example 2: Operational Context

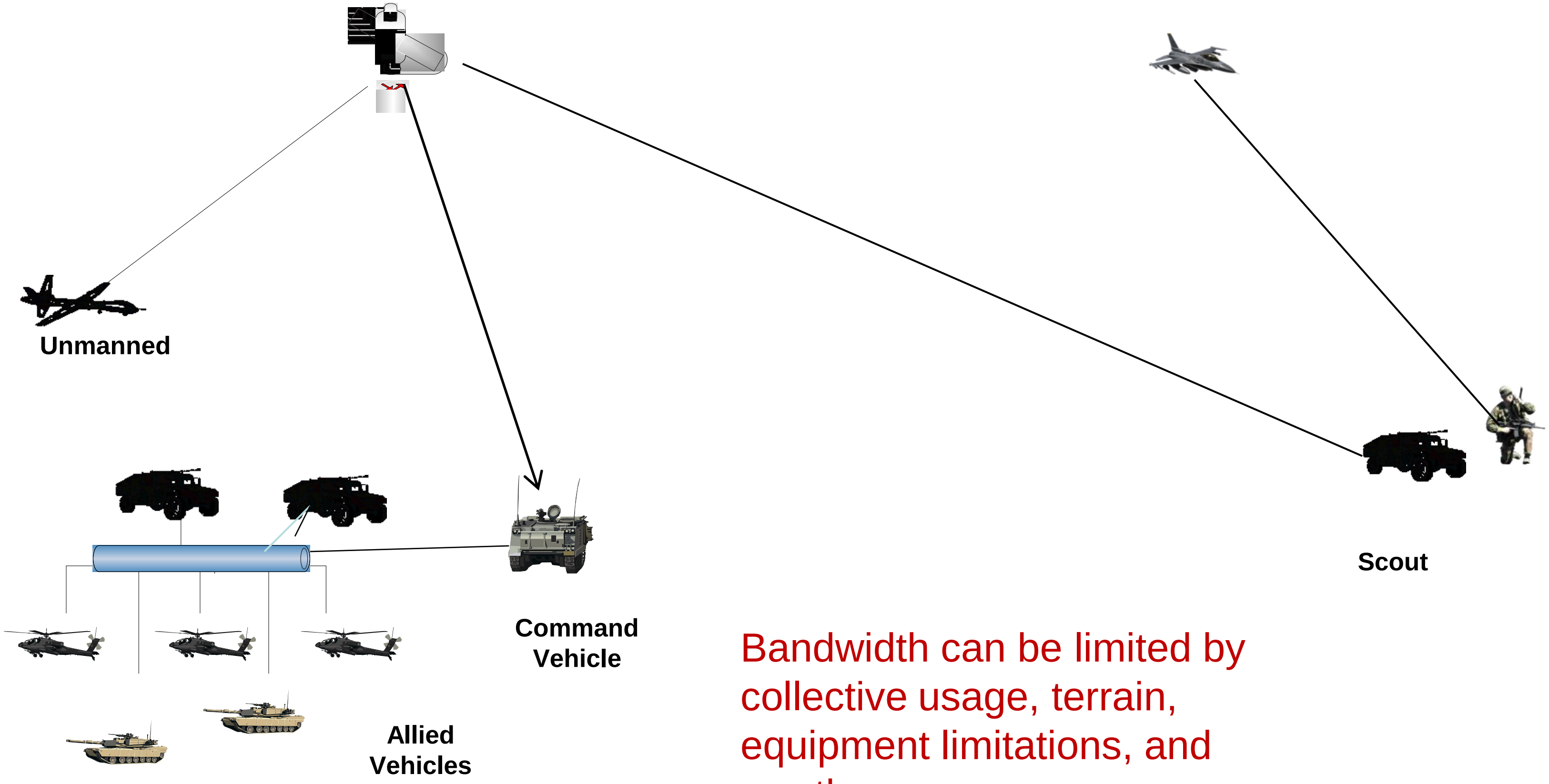
Mixture of communication mechanisms with high degradation potential

Wide spectrum of failure potentials (battle operations)

Wider spectrum of stakeholders (with potentially conflicting needs)

Multiple systems and their interactions (each participant is independent operator participating in system of systems)

Example 2: Mission Interactions



Bandwidth can be limited by collective usage, terrain, equipment limitations, and weather.

Example 2: Describing a Critical Step

Step 9	**Target Attack**
Precondition	Communication between JTAC and aircraft established Communication between JTAC and Army Target, friendlies, etc are “marked” appropriately
Action	Army approval: The supported army ground unit provides approval to the JTAC to release the weapons. Synchronization of target identification JTAC provides target corrections to aircrews as needed JTAC clears or aborts aircraft to attack
Post-Condition	Target is attacked

Example 2: Mission Critical Resource

Evaluate changes to a mission critical resource in Step 9

- JTAC and Aircraft establish secure communications

Potential resource context changes over time

- Currently voice, line of site (LOS)
- Enhanced to text and voice, LOS with satellite backup
- Expanded to satellite image sharing from UAV to JTAC and JTAC to aircraft

Example 2: Critical Resource Impact Evaluation

Failure impact potential:

- High: mission abort, mission errors with fratricide, wrong target
- Medium: mission delays; insufficient attack power; loss of IA for mission (exposure)
- Low: future mission potential

Selected failures for JTAC to aircraft communication (changes)

- Failure of communication connection – high impact (reduced with satellite backup)
- Partial transmission (retry required) – medium impact (increases with more channels – using more bandwidth)
- Encryption failure for communication – medium impact (unchanged)
- Incompatible communication software – medium to high impact (increases)

Example 2: Failure Analysis

For each failure option:

- Outcome for resource if failure realized (disclosure, modification, loss/destruction, unavailable)
- Impact on mission of compromised resource
- Impact rating (high, medium, low)
- Mitigations
- Response strategy (accept, monitor, mitigate)

Changes to system and software requirements resulting from decisions to mitigate

Polling Question 4

Do you consider the potential of operational failure when evaluating technology changes?

a) Yes

b) No

Multi-View Decision Making (MVDM)

Provides an approach that addresses the breadth and depth of activities, decisions, and products that must come together to successfully address complex software development

Evaluate and compare the mission, the integrated operational execution, and acquisition

- Mission-Oriented Success Analysis and Improvement Criteria (MOSAIC)
- Survivability Analysis Framework (SAF)
- System of Systems Interoperable Acquisition

Using SAF with Other Analysis Techniques

Security Assurance Case

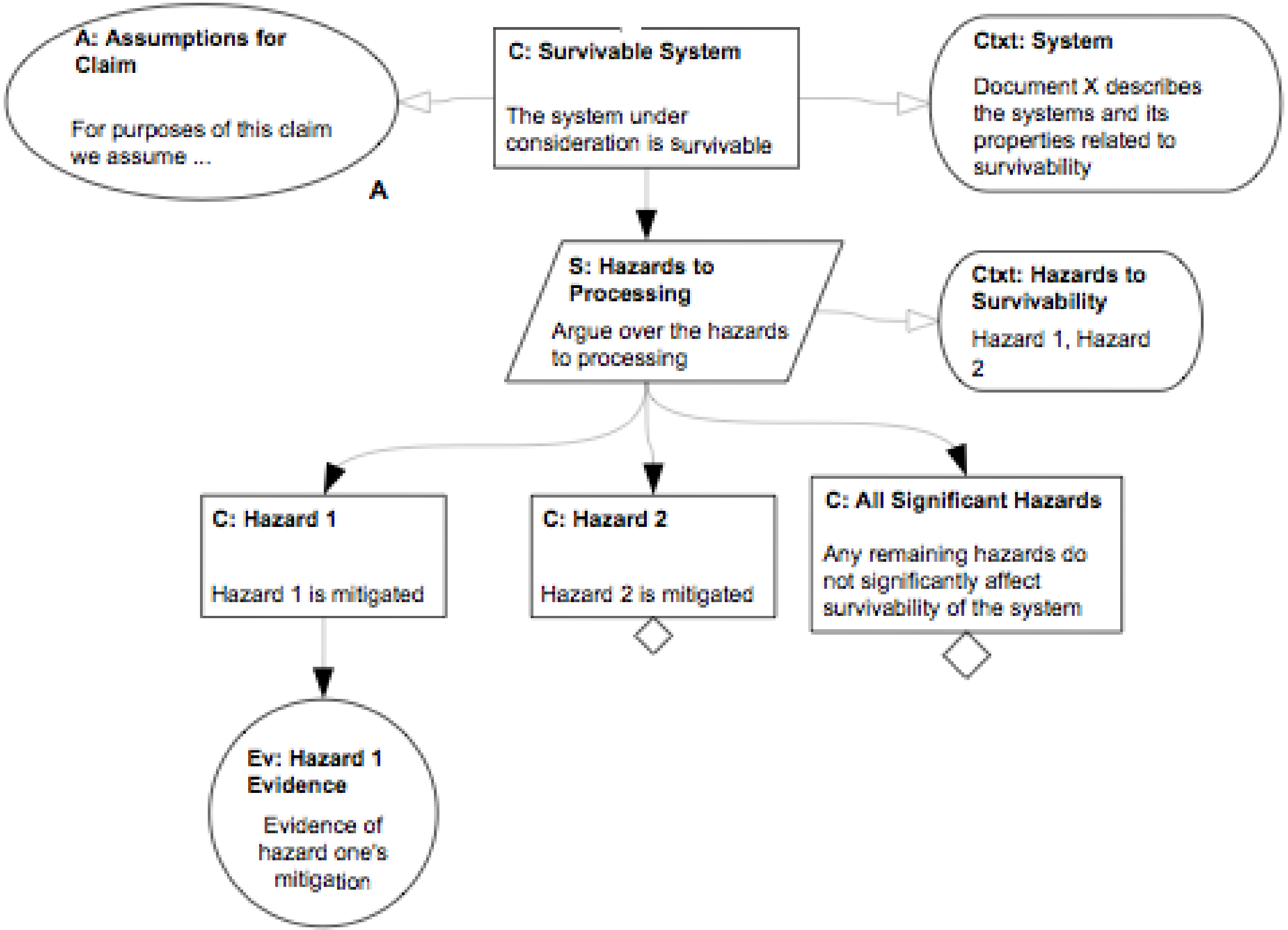
Structured view (claims, arguments, and evidence) that describes how potential security failures are addressed

- Connects mitigations with the threats they are addressing
- Identifies assurance gaps (missing evidence of mitigations)

Example Claim: Supplier follows suitable security coding practices

- Sub-claim: Supplier bans and enforces the ban on use of dangerous application programming interfaces
- Sub-claim: Static analysis tools with appropriate vulnerability coverage are applied at appropriate times throughout development
  - Evidence: Percentage of current code subject to static analysis
  - Evidence: Listing of applicable coding weaknesses
  - Evidence: Percentage of applicable coding weaknesses covered

Assurance Case Structure


A: Assumptions for Claim
For purposes of this claim we assume ...
A
C: Survivable System
The system under consideration is survivable
Ctxt: System
Document X describes the systems and its properties related to survivability
S: Hazards to Processing
Argue over the hazards to processing
Ctxt: Hazards to Survivability
Hazard 1, Hazard 2
C: Hazard 1
Hazard 1 is mitigated
C: Hazard 2
Hazard 2 is mitigated
C: All Significant Hazards
Any remaining hazards do not significantly affect survivability of the system
Ev: Hazard 1 Evidence
Evidence of hazard one's mitigation

Summary

Use SAF to Plan for Survivability

Plan for normal operation and failure response

- Develop range of mission threads that are critical for normal operations
- Identify critical mission activities, participants, and resources
- Evaluate the range of unexpected behaviors that could contribute to mission failure
- Mitigate potential failure

Plan for operational mission impact of technology changes

- Identify critical mission resources affected by proposed changes
- Evaluate the operational impact of failures in the current and changed operational context
- Identify change requirements based on mitigations for survivability

Questions?

References

Ellison, R., Goodenough, J., Weinstock, C., and Woody, C. Survivability Assurance for Systems of Systems, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2008-TR-008, http://www.sei.cmu.edu/publications/documents/08.reports/08tr008.html

Alberts, C., Smith II, J., and Woody, C. *Multi-view Decision Making (MVDM) Workshop*, Software Engineering Institute, Carnegie Mellon University , CMU/SEI-2008-SR-035, http://www.sei.cmu.edu/publications/documents/08.reports/08sr035.html

Alberts, C.and Woody, C., “Consider Operational Security Risk During System Development” published in IEEE Security & Privacy January/February 2007

NO WARRANTY

Contact Information

Carol Woody, Ph.D.

Senior Technical Staff

CERT

Telephone: +1 412-268-9137

Email: cwoody@cert.org

U.S. mail:

Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

World Wide Web:

www.sei.cmu.edu

www.sei.cmu.edu/contact.html

Customer Relations

Email: customer-relations@sei.cmu.edu

Telephone: +1 412-268-5800

SATURN 2010

Sixth Annual SEI Architecture Technology
User Network Conference

ARCHITECTING FOR CHANGE

May 17-21, 2010
Minneapolis, Minnesota

CALL FOR PAPERS → www.sei.cmu.edu/saturn/2010

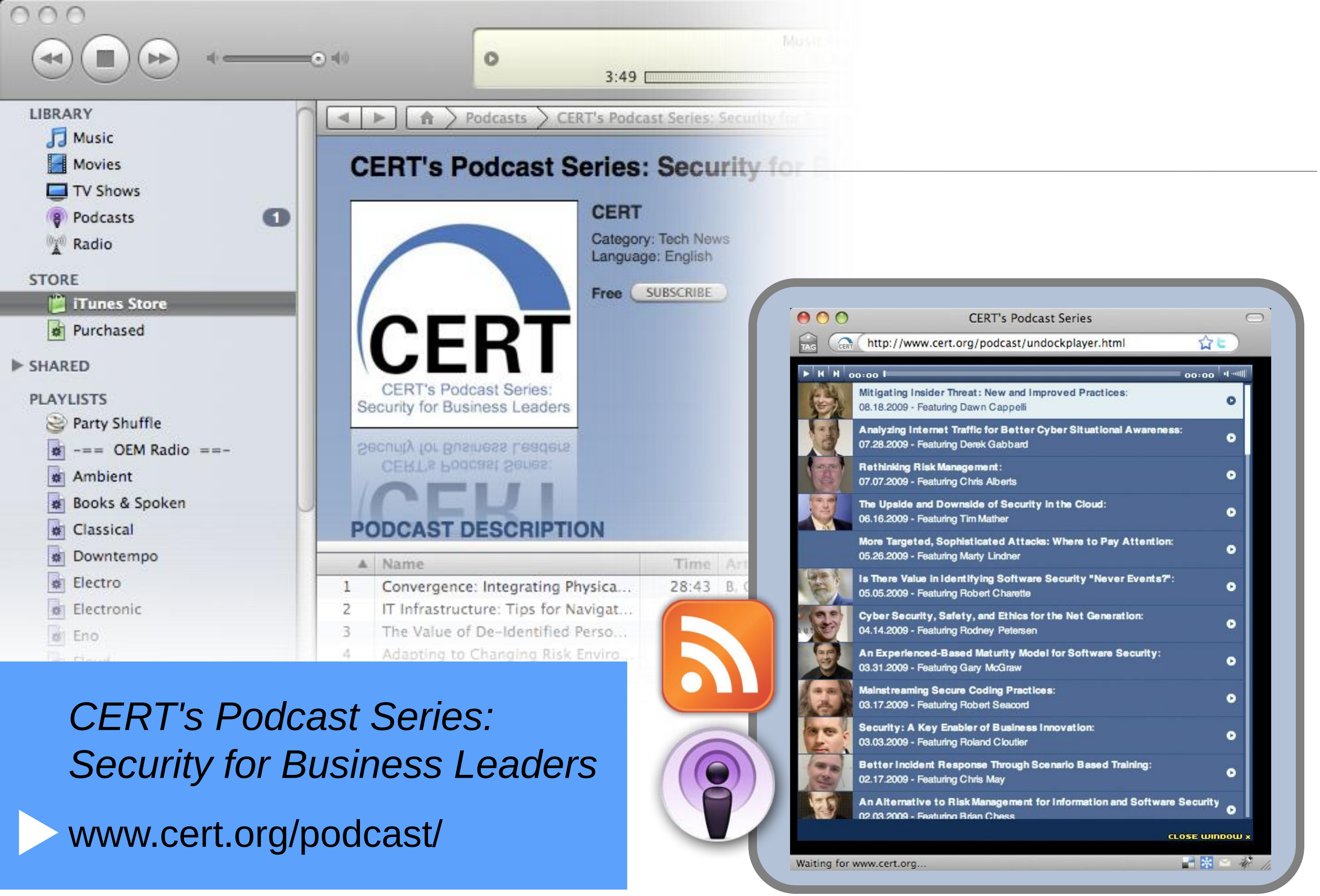
SEPG℠ 2010
NORTH AMERICA
Perform at a Higher Level

SEPG North America 2010

March 22–25, 2010
Savannah, Georgia

→ www.sei.cmu.edu/sepg/na/2010

SEPG is the premier, global conference series on software and systems process management



CERT's Podcast Series: Security for B

CERT

Category: Tech News
Language: English

CERT's Podcast Series: Security for Business Leaders

	Name	Time	Art
1	Convergence: Integrating Physica…	28:43	B. (
2	IT Infrastructure: Tips for Navigat…		
3	The Value of De-Identified Perso…		
4	Adapting to Changing Risk Enviro…		

CERT's Podcast Series

http://www.cert.org/podcast/undockplayer.html

Mitigating Insider Threat: New and Improved Practices:
08.18.2009 - Featuring Dawn Cappelli

Analyzing Internet Traffic for Better Cyber Situational Awareness:
07.28.2009 - Featuring Derek Gabbard

Rethinking Risk Management:
07.07.2009 - Featuring Chris Alberts

The Upside and Downside of Security in the Cloud:
06.16.2009 - Featuring Tim Mather

More Targeted, Sophisticated Attacks: Where to Pay Attention:
05.26.2009 - Featuring Marty Lindner

Is There Value in Identifying Software Security "Never Events?":
05.05.2009 - Featuring Robert Charette

Cyber Security, Safety, and Ethics for the Net Generation:
04.14.2009 - Featuring Rodney Petersen

An Experienced-Based Maturity Model for Software Security:
03.31.2009 - Featuring Gary McGraw

Mainstreaming Secure Coding Practices:
03.17.2009 - Featuring Robert Seacord

Security: A Key Enabler of Business Innovation:
03.03.2009 - Featuring Roland Cloutier

Better Incident Response Through Scenario Based Training:
02.17.2009 - Featuring Chris May

An Alternative to Risk Management for Information and Software Security
02.03.2009 - Featuring Brian Chess

CERT's Podcast Series:
Security for Business Leaders

▶ www.cert.org/podcast/

Become an SEI Member!

▶ www.sei.cmu.edu/membership

SEI Training

▶ www.sei.cmu.edu/training